

Metaanalysis of pseudorandom number generators

Tamás Herendi*, Viktória Padányi*

Department of Computer Science,
Faculty of Informatics University of Debrecen
Debrecen, Hungary

tamas.herendi@inf.unideb.hu, padanyi.viktoria@inf.unideb.hu

Abstract

Pseudorandom number generators are often used in solving different theoretical and practical problems. The particular applications expect generators having appropriate properties. The most important general properties are the following: the period length, the usability, the speed of calculation and if there is any implementation available or downloadable for the certain generator. In terms of usage, the qualities of the given generators are another interesting issue, which can be measured by statistical tests. Based on the above listed properties, the most suitable pseudorandom number generators can be selected depending on the application. We have collected some of the most well known pseudorandom number generators with uniform distribution and studied the significant properties they have. Furthermore, we have observed the principal properties which may be important for particular applications. Generators are reviewed from the classical (early) to the modern ones with special purpose. The classification of the generators is based on their properties and statistical tests. Finally, the collected quantified results are summarized.

MSC: 11Z05, 11K45, 65C10, 91A60

Keywords: pseudorandom number generators, statistical tests, uniformly distributed sequences, comparison of pseudorandom number generators

*This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was supported by the European Union, co-financed by the European Social Fund.